

CLAIMS

1. A method of managing meta data in a computing device, the method comprising the steps of:

5 collecting meta data resulting from use of the computing device, the meta data including application data usable in an application and context data for identifying context in which the application data are used;

determining statistical information associated with the meta data, the statistical information indicating relationships between the meta data;

10 storing the meta data and the statistical information in a storage of the computing device; and

retrieving, from the storage, application data that would be most appropriate for a current context of using the application based on the context data and the statistical information.

15 2. The method of claim 1, further comprising the step of:

applying the retrieved application data in the current context.

20 3. The method of claim 1, wherein the context data identify at least one of the following: user roles, uniform resource identifiers (URIs), file names, and/or form names pertaining to the application data.

25 4. The method of claim 1, wherein the application data include at least one of the following: page display setting data, file display setting data, user ID/password combinations, field values for computer forms, user's preference data, bookmarks, and authentication data.

30 5. The method of claim 4, wherein the authentication data include at least one of the following: certificates, or public keys.

6. The method of claim 1, wherein the meta data are stored in (key, value) pairs.

7. The method of claim 1, wherein the statistical information indicates frequencies in which particular application data are used together in particular contexts.

5

8. The method of claim 1, wherein the computing device implements a Common Data Security Architecture (CDSA), and the retrieving step is performed by a CDSA add-on module.

1005159-0130

10 9. The method of claim 1, wherein the current context includes at least one of the following: opening a web page, filling in a computer form, filling in a password-changing form, providing a certificate, opening a computer file, or processing a computer file, or executing an application program.

15 10. The method of claim 1, further comprising the step of:
providing a graphical user interface (GUI) for allowing the user to organize the stored meta data.

20 11. The method of claim 10, wherein the GUI displays a graphical tool in a cylindrical configuration for organizing the stored meta data.

12. The method of claim 1, wherein the retrieving step is performed using heuristics algorithms.

25 13. The method of claim 1, wherein the retrieving step includes the steps of:
formulating search requirements based on the current context of using the application; and
executing a search based on the search requirements.

30 14. The method of claim 13, wherein the search requirements specify weighted properties of the current context of using the application.

15. The method of claim 14, further comprising the steps of:
applying the retrieved application data in the current context; and
applying predetermined application data in the current context if no such most
appropriate application data are retrieved in the retrieving step.

5

16. The method of claim 1, wherein the current context is for filling in a computer
form, and the method comprises the step of:
automatically filling in the computer form with said most appropriate
application data.

10

17. The method of claim 16, further comprising the steps of:
retrieving, from the storage, alternative application data that are related to the
current context of filling in the computer form; and
presenting the alternative application data to a user for the user's
consideration.

15

18. The method of claim 16, wherein the computer form is a password-changing
form, and the retrieved application data include a user identification and a password.

20

19. The method of claim 18, wherein the filling step includes the steps:
presenting the password in the form in an obfuscated format;
determining whether it is safe to present the actual password to a user; and
presenting the actual password in a non-obfuscated format when it is
determined to be safe to present the actual password.

25

20. The method of claim 19, wherein the step of determining whether it is safe to
present the actual password is performed based on input from the user.

21. The method of claim 19, further comprising the step of:
replacing the password stored in the storage with a new password if the new
password has been accepted by a receiving party.

30

22. A computer program product embodied on computer readable medium readable by a computing device, for managing meta data in the computing device, the computer program product comprising computer executable instructions for:

5 collecting meta data resulting from use of the computing device, the meta data including application data usable in an application and context data for identifying context in which the application data are used;

determining statistical information associated with the meta data, the statistical information indicating relationships between the meta data;

10 storing the meta data and the statistical information in a storage of the computing device; and

retrieving, from the storage, application data that would be most appropriate for a current context of using the application based on the context data and the statistical information.

15 23. The computer program product of claim 22, further comprising computer executable instructions for:

applying the retrieved application data in the current context.

20 24. The computer program product of claim 22, wherein the context data identify at least one of the following: user roles, uniform resource identifiers (URIs), file names, and/or form names pertaining to the application data.

25 25. The computer program product of claim 22, wherein the application data include at least one of the following: page display setting data, file display setting data, user ID/password combinations, field values for computer forms, user's preference data, bookmarks, and authentication data.

30 26. The computer program product of claim 25, wherein the authentication data include at least one of the following: certificates, or public keys.

27. The computer program product of claim 22, wherein the meta data are stored in (key, value) pairs.

28. The computer program product of claim 22, wherein the statistical information indicates frequencies in which particular application data are used together in particular contexts.

29. The computer program product of claim 22, wherein the computing device implements a Common Data Security Architecture (CDSA), and the computer program product is implemented as a CDSA add-on module.

30. The computer program product of claim 22, further comprising computer executable instructions for:

updating the computing device with meta data resulting from use of the computing device in the current context.

31. The computer program product of claim 22, wherein the current context includes at least one of the following: opening a web page, filling in a computer form, filling in a password-changing form, providing a certificate, opening a computer file, processing a computer file, or executing an application program.

32. The computer program product of claim 22, further comprising computer executable instructions for:

providing a graphical user interface (GUI) for allowing the user to organize the stored meta data.

33. The computer program product of claim 32, wherein the GUI displays a graphical tool in a cylindrical configuration for organizing the stored meta data

34. The computer program product of claim 22, wherein the computer executable instructions for retrieving the most appropriate meta data is implemented using

heuristics algorithms.

35. The computer program product of claim 22, wherein the computer executable instructions for retrieving the most appropriate meta data includes computer

5 executable instructions for:

formulating search requirements based on the current context of using the application; and

executing a search based on the search requirements.

10 36. The computer program product of claim 35, wherein the search requirements specify weighted properties of the current context of using the application.

37. The computer program product of claim 36, further comprising computer executable instructions for:

15 applying the retrieved application data in the current context; and

applying predetermined application data in the current context if no such most appropriate application data are retrieved.

20 38. The computer program product of claim 22, wherein the current context is for filling in a computer form, and the computer program product comprises computer executable instructions for:

automatically filling in the computer form with said most appropriate application data.

25 39. The computer program product of claim 38, further comprising computer executable instructions for:

retrieving, from the storage, alternative application data that are related to the current context of filling in the computer form; and

30 presenting the alternative application data to a user for the user's consideration.

40. The computer program product of claim 38, wherein the computer form is a password-changing form, and the retrieved application data include a user identification and a password.

5 41. The computer program product of claim 40, wherein the computer executable instructions for filling in the computer form include computer executable instructions for:

presenting the password in the form in an obfuscated format;

determining whether it is safe to present the actual password to a user; and

10 presenting the actual password in a non-obfuscated format when it is determined to be safe to present the actual password.

42. The computer program product of claim 41, wherein the computer executable instructions for determining whether it is safe to present the actual password is
15 executed based on input from the user.

43. The computer program product of claim 41, further comprising computer executable instructions for:

20 replacing the password stored in the storage with a new password if the new password has been accepted by a receiving party.

44. A system for managing meta data in a secure manner, the system comprising:

25 a computing device capable of communicating with other communication devices through a communications network, the computing device including,
a plurality of applications selectably executable on the computing device,

a security architecture for selectively providing security-based services to at least one of the plurality of applications,

30 a data repository module, provided as an add-in module to the security architecture, for collecting meta data resulting from use of the computing device, the

meta data including application data usable in an application and context data for identifying context in which the application data are used, determining statistical information associated with the meta data, the statistical information indicating relationships between the meta data, storing the meta data and the statistical information in a storage of the computing device, and retrieving, from the storage, application data that would be most appropriate for a current context of using the application based on the context data and the statistical information.

45. The system of claim 44, wherein the data repository module includes:
the storage for storing the meta data;
a first interface for managing a process of storing the meta data in the storage; and
a second interface for retrieving from the storage said most appropriate meta data for the current context.

46. The system of claim 45, wherein the second interface formulates search requirements based on the current context of using the application, and executes a search based on the search requirements to retrieve said most appropriate meta data.

47. The system of claim 46, wherein the search requirements specify weighted properties of the current context of using the application.

48. The system of claim 44, wherein the context data include at least one of the following: user roles, uniform resource identifiers (URIs), file names, or form names pertaining to the meta data.

49. The system of claim 44, wherein the meta data are stored in (key, value) pairs.

50. The system of claim 44, wherein the security architecture is Common Data

Security Architecture (CDSA).

51. The system of claim 44, wherein the meta data represent at least one of the following: web page settings, file display settings, user ID/password combinations,
5 computer form data, user's preferences, book marks, and authentication data.

52. The system of claim 51, wherein the authentication data include at least one of the following: certificates, or public keys.

10 53. The system of claim 44, wherein the current context includes at least one of the following: opening a web page, filling in a computer form, filling in a password-changing form, providing a certificate, opening a computer file, processing a computer file, or executing an application program.

15 54. The system of claim 44, further comprising:
a meta data editor for providing a graphical user interface (GUI) that allows the user to organize the stored meta data.

20 55. The system of claim 54, wherein the GUI is a graphical tool in a cylindrical configuration.